THE ORGANIZATIONAL ANOMALY OF US ARMY STRATEGIC COUNTERINTELLIGENCE

A thesis presented to the Faculty of the US Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

MERLE V. BICKFORD, MAJ, USA
B.A., Union College, Schenectady, New York, 1984

Fort Leavenworth, Kansas
2003

Approved for public release; distribution is unlimited.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
06 JUN 2003		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Organizaitonal anomaly of US Army strategic counterintelligence	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Merle Bickford	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
US Army Command and General Staff College,1 Reynolds Ave,Fort Leavenworth,KS,66027-1352	**ATZL-SWD-GD**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The US Army conducts counterintelligence and law enforcement operations consistent with the laws and procedural statutes that govern these same operations in the US Air Force, US Navy, and the Federal Bureau of Investigation. Yet the Army has divided these investigative responsibilities under two separate and distinct organizations, thereby creating an organizational anomaly within the national strategic framework. Because law enforcement and American strategic counterintelligence activities serve as the principal means by which the nation protects its citizens and ensures national security abroad, it is important to acknowledge this anomaly and understand its ramifications. Effective collaboration between law enforcement and counterintelligence forces has been and will continue to be critical to national interests. This thesis explores the effectiveness of the Army's strategic organization for counterintelligence as overlaid on the theoretical and practical underpinnings of strategic Army intelligence, counterintelligence, and law enforcement. By incorporating this research with interview results, this thesis examines whether or not an intelligence organization is the most effective organizational construct for the prosecution of the Army's strategic, domestic counterintelligence mission and concludes with a broad examination of the strengths and weaknesses of the Army counterintelligence sociotechnical system in a modern context.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**1**	**63**	

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ Merle V. Bickford

Thesis Title: Organizational Anomaly of US Army Strategic Counterintelligence

Approved by:

_____, Thesis Committee Chair
LTC Yvonne Doll, M.S.

_____, Member
LTC James Burcalow, B.A.

_____, Member
Roger J. Spiller, Ph.D.

Accepted this 6th day of June 2003 by:

_____, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the US Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

THE ORGANIZATIONAL ANOMALY OF US ARMY STRATEGIC COUNTERINTELLIGENCE, by MAJ Merle V. Bickford, 57 pages.

The US Army conducts counterintelligence and law enforcement operations consistent with the laws and procedural statutes that govern these same operations in the US Air Force, US Navy, and the Federal Bureau of Investigation. Yet the Army has divided these investigative responsibilities under two separate and distinct organizations, thereby creating an organizational anomaly within the national strategic framework.

Because law enforcement and American strategic counterintelligence activities serve as the principal means by which the nation protects its citizens and ensures national security abroad, it is important to acknowledge this anomaly and understand its ramifications. Effective collaboration between law enforcement and counterintelligence forces has been and will continue to be critical to national interests. This thesis explores the effectiveness of the Army's strategic organization for counterintelligence as overlaid on the theoretical and practical underpinnings of strategic Army intelligence, counterintelligence, and law enforcement. By incorporating this research with interview results, this thesis examines whether or not an intelligence organization is the most effective organizational construct for the prosecution of the Army's strategic, domestic counterintelligence mission and concludes with a broad examination of the strengths and weaknesses of the Army counterintelligence sociotechnical system in a modern context.

TABLE OF CONTENTS

TABLES

ACRONYMS

BNL	Banco Nazionale de Lavoro
CI	Counterintelligence
CIA	Central Intelligence Agency
CID	Army Criminal Investigations Command
DHS	Defense HUMINT Service
DoD	Department of Defense
DSS	Defense Security Service
EO	Executive Order
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence and Surveillance Act of 1978
GAO	Government Accounting Office
HPSCI	House of Representatives Permanent Select Committee on Intelligence
HUMINT	Human Intelligence
LE	Law Enforcement
NCIS	Naval Criminal Investigative Service
OSI	Air Forces Office of Special Investigations
R&D	Research and Development.

CHAPTER 1

INTRODUCTION

The responsibilities for conducting the US Army's strategic, domestic counterintelligence (CI) and domestic criminal law enforcement (LE) functions are shared by two separate and distinct Army organizations, essentially dividing the responsibilities to prosecute legal investigations of different violations of *US Code* and the *Uniform Code of Military Justice*. The US Army's Criminal Investigation Command prosecutes all serious LE investigations for the Army (United States Army Criminal Investigation Command, 2002), while the US Army's Intelligence and Security Command oversees and prosecutes all Army CI investigations as well as conducts strategic intelligence operations for the Army (Intelligence and Security Command 2002). From its origin in 1939 as the Counter Intelligence Corps (Mendelsohn 1989) to its present organization under the Intelligence and Security Command, the Army's strategic CI unit has always been assigned to a command or intelligence organization separate from any LE organization (McDonough 1987). The fact the Army's strategic CI responsibilities are currently assigned to an intelligence organization is a facet of the anomaly of Army CI operations that bears potential repercussions specific to the Army alone. The fact that Army CI and LE responsibilities are not executed by the same US Army command and organization represents yet another, more significant, facet of the anomaly of Army CI operations, and this facet affects the entire national strategic CI-LE apparatus. The research conducted for this paper examines these anomalies and identifies

the help or hindrance they transfer onto the fundamental, strategic CI tasks of identifying espionage, investigating espionage, and neutralizing espionage.

The reason the Army's organizational approach to CI and LE investigative functions can impact the entire national CI-LE apparatus has to do with the common organizational nature of the remainder of the country's strategic CI and LE community. In the US Air Force, the Office of Special Investigations (OSI) investigates both criminal and espionage issues involving Air Force personnel (Air Force Office of Special Investigations 2000). The Naval Criminal Investigative Service (NCIS) has a similar role in that it enjoys sole jurisdiction of criminal and espionage issues within the Department of the Navy, to include the Marine Corps (Naval Criminal Investigative Service 2002). Similar to OSI and NCIS, the Federal Bureau of Investigation (FBI), as the enforcement arm of the Department of Justice, exercises Federal jurisdiction over instances of significant crimes and espionage within our nation's borders and is increasingly gaining overseas jurisdiction for significant criminal matters (FBI 2002; House of Representatives Permanent Select Committee on Intelligence [HPSCI] 1996). Because sister services and the FBI have clearly relegated their CI investigative responsibilities to those same organizations that manage their LE investigative responsibilities, the US Army's current organizational separation of LE and CI jurisdictions means that joint investigations between the Army and another service or the FBI, can require two Army investigators instead of just one. While this circumstance may appear trivial, neglecting to involve both representatives in joint investigations which require both investigative functions can have serious consequences, possibly resulting in investigative or litigation failures (McDonough 1987; Rindskopf-Parker 2000). This argument could represent the

basic argument against separating CI and LE investigative functions. Yet on the other hand, there is evidence to suggest that organizations that combine LE and CI investigative functions tend to devolve into primarily LE organizations. Before 11 September 2001, the FBI only had 25 percent of its agents working on CI and counterterrorism issues (The Brookings Institution 2002), and in effect practiced the culture of an intelligence-deficient LE organization (HPSCI 2002; Markle Foundation Task Force 2002). Since 11 September 2001, the FBI has reversed its investigative emphasis and has placed counterterrorism and CI at the top of its mission priorities (Mueller 2002; Szady 2002).

To understand the differences in organizational approaches to strategic CI and LE investigative functions, and the strengths and weaknesses of each form-to-function approach, a fundamental understanding of intelligence, CI, and LE can be helpful. The Department of Defense (DOD) Joint Publication (JP) 2.0 (2000) defines intelligence as: "1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding" (GL5). By this definition, intelligence can be seen as predominantly a proactive, offensive endeavor that, by nature, is designed to identify activities that have happened or will happen to enhance efforts or indices to determine policy or action (Brookings Institution 2002). To this end, the sources and methods of intelligence collection are generally encouraged to continue as long as possible and are carefully guarded to ensure the safety of sources and the continued viability of the operation (Thomas 1983). DOD JP 2.0 defines CI as: "1. Information

gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities" (GL3). Accordingly, CI agents investigate indications of espionage and terrorism to determine vulnerabilities and neutralize the spies or terrorists. This definition clearly places CI in a more reactive role, similar to LE situations where agents respond to a suspected crime or known crime for the purpose of neutralizing the criminals; however, CI generally differs from LE in the fundamental contexts of the investigative activities.

CI agents generally know who the spy is, but have to monitor how he or she is committing espionage and for whom he or she is spying before neutralization. The context for LE agents is normally contrary in that they know a crime was committed but must prove how and who actually did it, without observing the same perpetrator commit repeated, subsequent crimes. Although it may be shown that the fundamental investigative skills sets for Army CI and LE agents are similar (McDonough 1987; McNamara 1985), this subtle difference in the nature of the definitions and theoretical contexts of the CI and LE investigative functions must be considered in any separation of their organizations. Furthermore, it must be acknowledged that, despite their differences, CI and LE have more in common with each other by being fundamentally reactive than either one has with intelligence operations which are inherently proactive (Markle Foundation Task Force 2002).

This theoretical and practical similarity between CI-LE and intelligence is perhaps more significant than the differing investigative interrogatives (for whom vs. who) characterizing the CI and LE functions, because this similarity defines the nature of the

particular investigative function and the rules and codes by which the agent executes the operations (Markle Foundation Task Force 2002). This similarity implies an inherent compatibility among CI and LE investigative functions and warns of a possible incompatibility of both with intelligence functions. For this reason, the Army's decision to house its CI investigative functions within an intelligence organization can be seen as a theoretical liability to both the CI and intelligence functions should an operational overlap occur in either side. The repercussions of the CI and LE organizational strategy of the entire national community take on even more serious possibilities when one considers the evolution of transnational threats.

Since the United States was attacked on 11 September 2001, the National Intelligence Community has been the target of national sympathy, disappointment and abject ridicule. LE and CI organizations have experienced the same defacing scrutiny as Americans struggle to understand how terrorists could have coordinated such an attack without being detected. The newly established Department of Homeland Defense and the subsequent passage of the Patriot Act (2001) has rekindled the debate concerning the boundaries of LE, CI, and intelligence, a debate which saw its last fervor in the 1970s (Buncher 1977). The results of the last debate were manifested in the passage of the Foreign Intelligence and Surveillance Act (1978), known by its acronym FISA, and a subsequent series of executive orders designed to restrain the authorities of domestic intelligence collection, culminating with the Presidential signing of Executive Order 12333 (1981). This order proscribed DOD collection on US citizens except when specifically authorized during the approval regimen, which was to typify future national and Defense Department CI investigations. With the intent to reinforce Fourth

Amendment rights, this Executive Order was punitive in nature and resulted in the creation of a cumbersome hierarchy of oversight within the Army to control and monitor all CI investigations involving any American citizen, resident alien or US corporation, despite the fact that this demographic group was the target of choice for foreign spy handlers working in the United States (Department of the Army [DA] 1984). Within ten years of the signing of Executive Order 12333 (1981) the world would see the genesis of globalization and the increase of transnational threats to America.

Globalization has been and continues to stress the CI capabilities of all CI organizations. Charged with the official mission of detecting, deterring, and neutralizing foreign intelligence threats to Army forces, secrets, and technologies, Army strategic CI forces have failed to adapt their operational strategy for success in the new global environment. Since the end of the Cold War, Army strategic CI forces have downsized dramatically, in tandem with the entire Department of Defense. Army CI responded to the reduction of its force by reducing service to most civilian contractor clients and focusing Army CI services on a client base that is almost exclusively comprised of Army organizations. Unfortunately, this *decrease* of Army CI services to the civilian contractor sector occurred concurrently with pronounced *increases* in foreign intelligence services' capabilities and subsequent targeting of American research and development (R&D) information.

Globalization and the forces that propel it have contributed greatly to the development of new foreign espionage capabilities and new foreign espionage appetites. Exacerbating this situation for the Army is the fact that current international appetites have increasingly indicated a taste for sensitive US defense R&D information. In 1999,

there were 227 reports of foreign collection attempts at civilian American defense contractor locations (Defense Security Service [DSS] 2000), an 83 percent increase from 1998 (DSS 1999). These statistics suggest that during the boom of globalization, key forces supporting and expanding the global environment were increasing overall corporate revenues at the expense of security. From security and technology perspectives, it is reckless to assume that foreign collection capabilities and appetites have not abated nor receded from their 1999 levels, because in a fatigued world economy it is more reasonable to assume that efforts to steal profit-engendering secrets would increase rather than decrease. At the same time in US history, the FBI noted alarming increases in transnational threats of cyber crime and terrorism against America (Freeh 1998).

Federal legislation that counters these transnational threats can be characterized by the FISA (1978), the Economic Espionage Act (1996) and the Antiterrorism and Effective Death Penalty Act (1996), and The Patriot Act (2001). Of these acts, the one that has been used almost on a daily basis in any investigative CI activity is the FISA (1978). It is important to understand the genesis and impact of this act on the national CI and LE apparatus in order to appreciate how the legal context for CI investigations differs significantly from that of its LE counterparts.

Since the domestic intelligence abuses of the 1970s (Bunchner 1977), numerous presidential directives have whittled away at the military's ability to conduct comprehensive CI investigations except under the authorities granted by the court established under the FISA of 1978 (Hamre 2000). In fact a 2001 report by the General Accounting Office (GAO) entitled *Coordination Within Justice On Counterintelligence Matters Is Limited* has indirectly shown the FISA court approval process has actually

enhanced national CI investigative authorities instead of limiting them. The GAO study showed that FISA court approval of investigative requests were consistent with the FISA itself in that requests needed only show that the requested invasive investigative techniques were requested and conducted to satisfy a fundamental intelligence need, not a criminal need. Furthermore, this FISA legal review and approval process for CI investigative techniques was shown to be less stringent and more permissive than the legal review and approval process for LE investigative techniques, whose approval processes must consistently withstand any challenge of violating a person's Fourth Amendment rights and the further legal scrutiny under the criteria of the Federal Rules of Criminal Procedure (GAO 2001). The GAO study concluded that Department of Justice coordination (i.e., LE coordination) on CI investigations was flawed at best, because FBI CI investigators were reluctant to involve Federal prosecutors for fear that prosecutorial coordination or advice might later imply the fundamental purpose of the FISA-approved warrant was not intelligence, but was for criminal (LE) purposes. This implication would presumably render evidence collected under the FISA (1978) as inadmissible, or worse, require future collection or investigative actions concerning the suspect to undergo the stringent request and approval reviews associated with all LE investigations.

Because most CI activities are charged with collecting on foreign and domestic terrorists and terrorism is a crime that could warrant the death penalty under the Antiterrorism and Effective Death Penalty Act (1996), not being able to coordinate with LE authorities in a CI FISA-approved investigation hampered the effective neutralization of this insidious threat within the nation's borders. On 18 November 2002, after the US Attorney General's appeal to the FISA court's interpretation of the Patriot Act (2001), a

Federal appellate court ruled that intelligence and information collected pursuant to the authorities of the FISA (1978) could be shared with law enforcement officials without fear of damaging or otherwise poisoning the utility of this information for use in a subsequent criminal trial (Ashcroft 2002). In addition to enhancing the value and utility of CI investigations of terrorists, the Patriot Act and the subsequent decision by the Federal appellate court has illuminated the traditional problems of collaboration between CI and LE activities within the American democracy. Until just recently, even in the FBI where CI and LE forces work side by side under the same organization, procedures and legislation have undermined effective CI and LE collaboration. Now that the appellate court decision has affirmed that FISA-obtained evidence can be used in criminal trials, the separation of CI and LE investigative functions can be interpreted as a needless and artificial obstruction to collaboration.

These struggles in the FBI, Congress, the Federal court system and the Department of Justice to resolve the dichotomy of investigative approval processes and authorities in America, while preserving democracy, underscores the complexities of the CI and LE functions and practices in the US Army. These same courts that review FBI FISA requests review Army FISA requests and requests for joint FISA warrants for investigations involving the FBI and sister armed services. Looking at just the simple division in the federal approval process for investigative authorities, the US Army's organizational division of CI and LE roles and functions appears to adapt quite well to the federal approval processes. The LE warrant approval process is followed by one organization while the CI, or FISA, warrant approval system is followed by another organization and no one organization's legal representatives have to deal with two

separate, complex federal processes. But contemporary organizational change theory mandates that organizations develop not only to enhance production or services, but also to compliment the environmental context (Harvey and Brown 2001; Daft 2001). It does an organization no good, and in fact threatens its relevancy, if the organization demonstrates it can make the best 8-track tape player in the least amount of time when there is absolutely no market or need for that particular product. Therefore, it is necessary to examine the anomaly of the US Army's structural approach to CI and LE functions within the more contemporary environmental context of terrorism and intelligence organizations within the American democratic framework.

The Army CI mission is one that, by definition, involves countering the threats of espionage and terrorism (DOD 2000), but Executive Order 12333 (1981) limits intelligence agency investigations of terrorists to foreign terrorists only. Therefore, Army CI agents, by virtue of the fact that they are affiliated with an intelligence organization and function, are authorized to investigate foreign terrorists in the US while Army CID is authorized to investigate domestic, or US citizen terrorists in the US (DA 1984; Pratt 2002). During the Cold War and before the expansion of transnational influence during globalization, this parochial division of terrorism was perhaps acceptable, but with the current proliferation of the terrorist threat, the Army may not be well postured to respond coherently. Sister services and the FBI are not as encumbered by a distinction between foreign and domestic terrorism, because the same agents exercise LE as well as CI authorities and can just as easily obtain a FISA warrant as a more traditional warrant. This is not the case with Army CI and CID, so clearly more coordination and collaboration are needed between the organizations if they are to remain separate and

distinct in the prosecution of the Army's investigative responsibilities toward terrorism specifically.

The organizational anomaly of Army strategic CI activities being conducted from within an intelligence organization and separate from Army LE activities takes on greater significance with a more robust appreciation of the national CI structure, the theoretical and practical natures of intelligence, CI and LE, an enhanced understanding of the current transnational threats to America, as well as a grasp of the legal underpinning of both LE and CI investigations in American democracy. This paper will identify the key literature available to identify this anomaly and support a closer examination of the question of whether or not the intelligence organization is the most effective organizational construct for the prosecution of the Army's strategic, domestic counterintelligence mission and responsibilities. Because the Army CI mission involves countering espionage as well as foreign terrorism (Pratt 2002), this study will define effective as facilitating the identification of spies or foreign terrorists, facilitating the investigation of these spies or foreign terrorists, and finally facilitating the neutralization of these spies or foreign terrorists. This study will not make conclusions concerning Army CI activities being conducted within a LE organization, or any training similarities between LE and CI agents. This study will not examine or consider CI activities purportedly conducted by the Defense HUMINT Service or US Postal Service. Furthermore this study will not attempt to determine the best organization for Army CI activities or why the Army anomaly even exists today. This study will only assess if the current strategic, domestic CI construct can be improved upon or if it remains viable and efficient in today's context. This study will conclude with a broad analysis of the sociotechnical construct of the

current Army CI organization to serve as a starting point for further studies that may strive to gauge the Army CI organizational culture's reaction to any changes that may be recommended by this study.

CHAPTER 2

LITERATURE REVIEW

The literature available for this study is of mixed relevance. There is a dearth of literature specifically studying strategic Army CI activities and organization, but there is sufficient literature on CI and LE in general, specifically as practiced by the FBI. Because Army CI investigations are prosecuted in accordance with the same rules of law and evidence as FBI CI investigations, this literature can be used to provide verifiable responses to some fundamental research questions posed by this effort, specifically concerning the complimentary and conflicting aspects of intelligence, CI and LE. Because this thesis study endeavors to identify the most effective umbrella organization for the Army's CI functions and responsibilities, either under an intelligence organization or a LE organization, understanding the intrinsic theoretical conflicts between intelligence, CI and LE is fundamental to this study's intent. Therefore the literature available provides the bedrock understanding of the issues while subsequent field work, as described in the subsequent chapter, will provide the data for the remainder of the research effort.

This chapter will review the key experiential, statutory and theoretical literature available at this date concerning the roles, responsibilities and functions of CI as they relate to those of LE. The literature reviewed is in agreement that fundamental differences in intelligence, CI and LE demand that collaboration between these elements require careful handling to avoid lapses of CI protections or there are predominantly two fundamental views on the most effective associations for CI and LE. The first of these

views proposes that organizations can remain distinct but should develop mechanisms that engender more productive collaboration. The other view posits the investigative functions should be combined under one headquarters and staff to enhance oversight and control. Each of these views proffers or directs mechanisms that appear poised to induce collaboration. The contrasting view proposes the organizations be combined for various reasons. The following paragraphs provide a discussion of the literature espousing these views.

Rindskopf-Parker (2000) believes that collaborative intelligence and law enforcement operations can be a significant weapon against the growing transnational threats to the US, but stresses that the blurred jurisdictional boundaries and history of misunderstanding between intelligence and law enforcement services inhibit developing a synergy conducive to successful prosecutions. She blames this misunderstanding on the fundamental differences in intelligence and law enforcement functions and responsibilities, based upon her insights gained while serving as General Counsel for the CIA and NSA and the senior legal adviser to the US Intelligence Community during the debacles encountered when national intelligence services were compelled to collaborate with domestic law enforcement forces in the Banco Nazionale de Lavoro (BNL) and the Clipper Chip cases. Rindskopf-Parker contends that an endemic misunderstanding of each others' capabilities and limitations, based upon the differing legal requirements which require segregation of certain efforts, are the primary reasons for the failure of intelligence and LE collaboration in these cases. In particular Rindskopf-Parker's work as legal co-chair investigating the BNL scandal, which involved the Department of Justice accusing the Central Intelligence Agency of deceit in an official LE investigation,

underscored her perspective of the magnitude of the divide in understanding and provides additional credibility to her writings. The BNL case involved the fraudulent movement of millions of dollars among US branches of an Italian bank. When the Department of Justice officially asked the Central Intelligence Agency (CIA) if it had any reports of "criminal" significance on the BNL case, the CIA's answer was a prompt negative because it understood that it was not permitted to collect law enforcement information to begin with, and as Rindskopf-Parker determined in her subsequent investigation, the CIA counsel was not equipped to recognize the criminal liabilities in the reports it did have because their lawyers were ostensibly trained only in intelligence law. When it was later discovered the CIA did have information helpful to the criminal prosecution of the BNL case, the accusations of lying and counteraccusations led to Rindskopf-Parker's appointment to determine the cause of these circumstances. As mentioned earlier, she found these circumstances to be an inherent proclivity of the national apparatus for prosecuting intelligence and LE operations. Her proposed solution to this proclivity is based on her personal, experience and observations, and is therefore relevant and extremely helpful to this thesis.

Rindskopf-Parker's (2000) contentions of the innate differences between intelligence and law enforcement can be characterized by the disparate treatment of sources. She underscores the fact that sources in intelligence operations are generally safeguarded and protected from disclosure to ensure their safety and the fidelity of reporting, whereas sources in law enforcement investigations are generally revealed at the first opportunity that disclosure can benefit the prosecution. This basic difference, in Rindskopf-Parker's experience, has resulted in misunderstandings among law

enforcement and intelligence professionals working under collaborative circumstances. Additionally, she contends that differences in intelligence and law enforcement functions and responsibilities are codified in US law and that some senior DOJ officials are not familiar with these differences. Due to the FISA of 1978 and Executive Order 12333 (1981), national and DoD intelligence services are prohibited from collecting on US persons which, according to Rindskopf-Parker, has effectively limited federal law enforcement activities to the continental US and Federal intelligence activities to overseas. Due to her involvement in the BNL case, she suggests that few of her DOJ counterparts understand this difference in Intelligence Law and Domestic/Criminal Law and further speculated that the gap in understanding is increasing. In her experience, she stated she has only identified reciprocal understanding of Intelligence Law by the DOJ in a few instances.

In those instances where an understanding of Intelligence Law was warranted and displayed by the DOJ in collaborative cases, Rindskopf-Parker (2000) points out this understanding was derived from experience on the part of the DOJ individual. For this reason, she concludes the best way to mitigate the current lack of collaboration is to require that key officials rotate assignments between intelligence and LE positions, ostensibly to afford greater exposure to the realms of intelligence law well as domestic law. Applying this solution to the Army CI-LE context, one can argue a common organization or common training for Army CI and LE agents may mitigate misunderstandings and operational inefficiencies currently experienced.

Another document that stresses the need for increased collaboration between LE and CI and Intelligence communities is the “IC21: The Intelligence Community of the

21st Century" staff study conducted by the HPSCI in 1996. This authoritative study also noted an increasing need for enhanced and effective CI and LE collaboration to counter the increasing transnational threats to national and domestic security. This document made specific recommendations concerning intelligence sharing while acknowledging the legal problems of law enforcement oversight of CI investigations. This report made no recommendations concerning structural changes to any intelligence, CI, or LE organizations, but did serve to highlight concern of a lack of meaningful, effective collaboration. It is interesting to note that, similar to the Rindskopf-Parker essay (2000), the IC21 report also referred to the BNL debacle as evidence that more collaboration is needed.

In 2001, President Clinton signed a Presidential Decision Directive entitled "US Counterintelligence Effectiveness - Counterintelligence for the 21st Century." This directive described specific steps intended to enhance the US CI community's ability to fulfill its mission of identifying, understanding, prioritizing and neutralizing the intelligence threats faced by the United States. The system prescribed the establishment of a CI Board of Directors that would manage an inter-agency hierarchy of working groups with the common goal of becoming more predictive, proactive and able to maintain integrated oversight of counterintelligence issues across the national security agencies. Because this interagency hierarchy was directed to be based upon a board of senior officials chaired by the Director, FBI and composed of the Deputy Secretary of Defense, Deputy Director of Central Intelligence and a senior representative of the Department of Justice, the directive can be seen as attempting to increase the amount of collaboration between intelligence, CI and LE agencies, to include those intelligence, CI

and LE agencies within the Department of Defense (National Counterintelligence Center 2002).

The key resources discussed above demonstrate a collective concern, at the highest levels of the nation's government, that CI and LE activities may not be as collaborative as necessary to defeat the magnitude of mounting transnational threats. These threats include espionage, that jeopardizes our national security as well as our industrial base, and terrorism. These threats in particular, as they affect the Army's personnel and secrets, are within the jurisdictional mission of Army CI. Without suggesting an overhaul of organizations whose missions are to counter these threats, the resources above only stressed better CI-LE collaborative mechanisms to enhance defeat of the threat.

A contrasting viewpoint to simple collaboration is provided by a master's thesis produced by T. McDonough (1987) for the US Army Command and General Staff College. His research concluded that Army CI and LE functions should be organized under a common agency. Without proposing that this agency be a LE or an intelligence agency, McDonough contends that CI investigations would be enhanced if more collaboration, at early stages, were facilitated by centralized command and control. McDonough supported his conclusions with selected case studies, field interviews, and references to a 1964 Department of the Army unclassified extract of a classified study entitled "Security Shield," which recommended more collaboration between Army CI and LE forces. The evidence presented by McDonough's study does support his conclusion, but could be accused of being too subjective and without basing his conclusions in theory. For that reason, and the fact that so much has changed within the

external and target environments of the Army CI organization since 1987, this study is needed to regain perspective on the Army's CI mission as it is complimented or defeated by its functional structure.

CHAPTER 3

RESEARCH METHODOLOGY

This study is concerned with a theoretical discussion of the natures of intelligence and CI and how these fundamental natures conflict or compliment the nature of LE. This study is also concerned with the practical application of intelligence, CI and LE, as these practices relate to the mission of Army strategic, domestic CI investigative functions of identifying, investigating and neutralizing foreign intelligence threats to the Army as well as identifying and collecting on foreign terrorist threats to the Army. Within the context of these concerns lies the primary question of this study which is an alchemic blend of the theoretical and practical. Is an intelligence organization the most effective organizational construct for the prosecution of the Army's strategic, domestic counterintelligence mission and responsibilities? Nested within this primary question are the following secondary questions: (1) Are there fundamental qualities of counterintelligence investigations and operations that characterize them as fundamentally law enforcement functions or intelligence functions? (2) Why is Army counterintelligence organization distinct from Army law enforcement organization? and (3) what are the specific criteria to measure the effectiveness of a counterintelligence effort? These secondary questions can only be fully answered by addressing a level of supporting tertiary level questions. These tertiary level questions are shown below along with the primary research method used to satisfy the question.

Secondary Question 1: Are there fundamental qualities of counterintelligence investigations and operations that characterize them as fundamentally law enforcement functions or intelligence functions?

a) How would law enforcement organization or functions facilitate the prosecution of Army counterintelligence investigations? This question will be primarily satisfied by results of interviews

b) How would law enforcement organization or functions hinder the prosecution of Army counterintelligence investigations? This question will be primarily satisfied through interview results.

Secondary Question 2: Why is Army counterintelligence organization separate from Army law enforcement organization?

a) Are the conditions that precipitated the segregation still valid today? This question will be satisfied primarily by literature.

b) How do sister services execute law enforcement and counterintelligence responsibilities within the same organization and what are the benefits and challenges/problems of their particular applications? This question will be satisfied primarily by interview results.

Secondary question 3: What are the specific criteria to measure the effectiveness of a counterintelligence effort? This question will be satisfied by McDonough's (1987) master's thesis.

This study's literature review found that literature on the Army CI construct is contemporarily deficient. In fact, only one study (from 1987) is available that addresses the research question of this study. Therefore, the interview phase of this research

endeavor will be of critical importance to discerning the true nature of the current benefits and hindrances of the Army's choice to house its CI investigative functions within an intelligence organization. The interview format for this research effort is presented below.

Interview text format

I am Major Merle Bickford of the US Army. I am an Army Counterintelligence (CI) Officer with approximately four years of operational experience in CI assignments in Panama and the US, to include 21 months of command of strategic CI investigators in the US

The purpose of this interview is to obtain information which will assist my master's thesis research. My research question concerns the feasibility and desirability of combining Army investigative functions which are currently conducted separately by the US Army Criminal Investigation Command and the US Army Intelligence and Security Command, under an arrangement similar to that of the Air Force Office of Special Investigations, Naval Criminal Investigative Service, or Federal Bureau of Investigation. I'm looking for data/input from key individuals currently prosecuting the Army's CI and law enforcement missions in order to support additional research and lead to a valid conclusion. This eventual conclusion could find that the Army is best served by maintaining the status quo and continuing to prosecute the Army's CI mission from within its intelligence organization, or that the Army could be better served by realigning its CI functions under another organization.

I intend to submit my thesis in unclassified form. I will phrase my questions in such a way as to allow for maximum flexibility in your response, but will only be able to record that which is unclassified. If you do have any concern about the classification of any of your responses, please let me know.

On questions concerning investigative effectiveness, I will address three criteria with you, namely detection of the subject, prosecution of the investigation pertaining to the subject, and neutralization of the subject. I remind you that I am only concerned with the Army's law enforcement and strategic CI investigative abilities and activities within the continental US

At the end of this interview I will review with you what I believe were your responses to ensure that I understood what you said and that you will understand what will be attributed to you in my final thesis research. If you wish me to limit your responses in any way, please let me know so that I may honor your requests and ensure these sections are removed from the record of this interview and not subsequently published. I will respect and honor your requests.

(QUESTIONS 1-5 FOR ALL PERSONNEL)

1. What is your name, rank, and grade?

2. What is your current (or last) operational duty assignment?

3. What military education have you received (concerning your specialty)?

4. What is your military (or civilian) career specialty code?

5. What military or civilian investigations-related jobs have you had?

(QUESTIONS 6-14 FOR NON-ARMY PERSONNEL)

6. Please briefly describe the mission and structure of your organization.

7. What is the relationship of counterintelligence and criminal investigations in your unit?

8. What common resources, if any, in both types of investigations?

9. What benefits and disadvantages do you see in the combination of the investigative missions?

10. Have you had any personal experience or first-hand knowledge of cases demonstrating the benefits or disadvantages of the combination of investigative missions?

11. Have you had any operational dealings with Army investigators? What element did you deal with and what was the nature and result of the contact? Were there any noticeable effects on the cooperation due to the Army's separation of investigative mission responsibilities? Were there any noticeable effects on the investigation's conduct because of the Army's separation of investigative mission responsibilities? If so, what were they?

12. What type of organizational approach do you believe to be the most effective in dealing with the military investigative mission, separate or combined? Why?

13. Does your unit's mission responsibilities include the collection of information regarding foreign terrorists within your jurisdiction? If so, is the information you collect reported through intelligence channels, law enforcement channels, or both?

14. Does your unit's mission responsibilities include the collection of information regarding domestic terrorists within your jurisdiction? If so, is the information you collect reported through intelligence channels, law enforcement channels, or both?

(QUESTIONS 15 – 26 FOR ARMY PERSONNEL)

15. What benefits and/or disadvantages do you see in a combination of the criminal and counterintelligence investigation missions under one agency?

16. Do you have any personal or first-hand knowledge of cases in which the benefits or disadvantages of such a combination have been demonstrated? If so, please give a brief description of the circumstances involved.

17. What benefits and/or disadvantages do you see in the continued separation of the criminal and counterintelligence investigation missions under two agencies?

18. Do you have any personal or first-hand knowledge of cases in which the benefits or disadvantages of the current separation have been demonstrated? If so, please give a brief description of the circumstances involved.

19. Have you noted any effects, either positive or negative, on the Army's ability to conduct counterintelligence investigations which can be attributed to the separation of its investigative missions?

20. Have you noted any effects, either positive or negative, on the Army's ability to conduct law enforcement investigations which can be attributed to the separation of its investigative missions?

21. What type of organizational approach do you believe to be the most effective in conducting Army law enforcement investigations? Why?

22. What type of organizational approach do you believe to be the most effective in conducting Army counterintelligence investigations? Why?

23. Do you believe that an intelligence organization is the most effective construct for the prosecution of the Army's CI mission and responsibilities? Why or why not? If not, what type of organization would be the most effective and why?

24. Does your unit's mission responsibilities include the collection of information regarding foreign terrorists within your jurisdiction? If so, is the information you collect reported through intelligence channels, law enforcement channels, or both?

25. Does your unit's mission responsibilities include the collection of information regarding domestic terrorists within your jurisdiction? If so, is the information you collect reported through intelligence channels, law enforcement channels, or both?

26. Have you ever conducted investigations with another Armed Service? If so, has the current separation of investigative jurisdictions in the Army helped or hindered your conduct of the investigation in any way? If so, how?

The organizational diagnosis portion of this study will involve a detailed examination of the Army CI organization, its advantages and disadvantages, as compared to other organizations performing similar functions. These advantages and disadvantages will be interpreted through the application of the contemporary sociotechnical model of organizational development (Harvey and Brown 2001). Without drawing any premature conclusions concerning a need for change of the Army CI organizational construct, the resulting diagnosis will gauge and catalogue the Army CI organization's strengths and weaknesses across the sociotechnical subsystems and the three fundamental CI tasks of identify, investigate, and neutralize.

CHAPTER 4

ANALYSIS

An analysis of the intricacies of the problem delineated in chapter 1 identified a national, strategic CI apparatus that has been controlled by a FISA court approval system acting independent from criminal rules of procedure since 1978. Chapter 1 discussion also underscored the relevance of the recent passing and interpretation of the Patriot Act (2001), which served to moderately erode the FISA barriers to collaboration previously existing between CI and LE agents and enhance abilities to counteract growing global espionage and terrorist threats. Chapter 1 discussion also showed how the theoretical tendencies of strategic CI investigations and operations were more aligned with LE investigations and operations than with intelligence operations, establishing the differences of reactive response in CI and LE versus the proactive tendency of intelligence. A key argument in chapter 2 concerned Rindskopf-Parker's (2000) conclusion that CI and LE forces were much more effective if cognizant of each other's operational strengths and limitations, proposing key leaders rotate between CI and LE positions to guarantee this mutual understanding. These preceding arguments, in the aggregate, suggest CI is a national activity which has been mechanically segregated from LE by the FISA, but which requires increasingly close collaboration with LE to meet the challenges of today's global context. This suggestion clearly has dramatic implications for Army CI. The Army segregation of CI and LE organizations may have suffered no detriment while the intermixing CI and LE information was prohibited by national policies and regulations, but now that such intermixing is no longer proscribed, the

segregation of the organizations may actually constrain the Army's ability to take advantage of Patriot Act (2001) permissions to collaborate. Therefore, before any analysis of the data collected in field interviews of Army and Air Force CI and LE personnel, the literature currently available implies an organizational fallibility intrinsic to the segregation of CI and LE functions and organizations in the Army. In order to gain a more comprehensive understanding of this fallibility, or perhaps identify some benefits to the Army approach not specifically delineated in available literature, it becomes necessary to examine the data from the interviews conducted.

In this analysis, the advantages and disadvantages of the Army's CI and Intelligence organizational model (the status quo) were compared to a hybrid CI-LE model which characterized the rest of the national CI architecture. The two models were then assessed in terms of their overall ability to satisfy the fundamental CI tasks of identifying, investigating and neutralizing the espionage as well as the foreign and domestic terrorist threats in a series of interview questions presented in Chapter 3 of this thesis. Perspectives from Army CI, Army LE, and two non-Army investigators with responsibility for both CI and LE were gathered in the course of this study. In some cases individual interview responses expressed clear advantages and disadvantages of both the Army CI and Intelligence organizational model as well as the CI-LE model. But in all cases, a bias toward one or the other was requested and received along with justification. It is interesting to note that of all organizations interviewed, the only organization which proffered a bias for the CI and Intelligence model, which represents the status quo, was the Army CI interviewee. All other interviewees expressed other biases for what each saw as a need for the CI-LE organizational construct. This chapter will present the gist of

each interview accompanied by a graphic representation of the advantages and disadvantages each interviewee saw with the CI and Intelligence and CI-LE models appropriately overlaid on one, two, or all three CI functions this study initially established as the measure of effectiveness for Army CI. At chapter's end, a synthesis of findings will be presented in a solitary chart.

The interview with the Army CI representative marked the first of the series of interviews and, as such, established some themes which were later noticed as common among other interviews and research. Some of these themes can be characterized as the following benefits from being part of an intelligence organization: access to a classified communications architecture that not only protects investigative correspondence, but permits access to national intelligence products that assist their target identification processes; the organization did not have the tendency to devolve into an LE culture and lose touch with the CI missions as seen with the FBI (Brookings Institution 2002); and the third benefit was rapid access to intelligence analysis capabilities during their investigations and neutralization phases. This last benefit is particularly lacking in FBI field offices (Brookings Institution 2002). For the purposes of this study, it is important to note at the time of this interview, the interviewee concurrently commanded Army CI investigative agency for one-third of the nation's domestic geography. The advantages of the CI and Intelligence and CI-LE organizational models articulated by this Army CI interviewee and described above are captured visually in table 1.

Table 1. Advantages of Organizational Models per Army CI Interviewee

	CI and Intelligence	**CI-LE**
Identification	National intelligence connectivity Singular focus	
Investigation	Access to intelligence analysis Specialized knowledge of complex rules Can perform intelligence collection missions	Investigates foreign and domestic terrorists
Neutralization	Intel analysis can aid LE agencies	Internal collaboration for most cases

Despite the preponderance of advantages, the interview with the Army CI representative also noted a disadvantage of being part of an intelligence organization, namely that Army CI relationships with LE agencies and industry were largely personality-dependent which could affect their capabilities in all phases of their CI process. Another disadvantage concerned the CI-LE model, which the interviewee opined had the habitual tendency to evolve a criminally focused organizational culture instead of a CI focused culture. While the former disadvantage was later noted as a common theme among other interviews, the latter was seen again in an OSI interview and in research literature (Brookings Institution 2002). It is possible the latter disadvantage was not seen again in other interviews, and thereby become thematic, was because all other interviewees were either part of an LE organization or a combined LE/CI organization to which the interviewee was referring. The disadvantages described above are visually displayed in table 2.

Table 2. Disadvantages of Organizational Models per Army CI Interviewee

	CI and Intelligence	**CI-LE**
Identification	Reliance on external LE coordination	Evolution of criminal-centric culture
Investigation	Reliance on external LE coordination	
Neutralization	Reliance on external LE coordination	

In reviewing the advantages and disadvantages of this interview of an Army CI representative, not only do the advantages of the CI and Intelligence model outnumber the disadvantages given, but other responses to interview questions clearly represented an interviewee bias toward that model. In summary, this interview highlighted that although Army CI was restricted from investigating domestic terrorists, because of executive order and regulations constraining military intelligence collection targeting US citizens, the Army CI culture was comfortable being an intelligence culture and felt that what it lacked in investigative jurisdiction it made up for with intelligence connectivity, analysis, and national intelligence contributions. This element of satisfaction with a contribution to the national intelligence effort was not apparent in other interviews and therefore remained a defining cultural characteristic of the CI and Intelligence organizational model in this study.

The only other interview of an Army investigator was of an operations officer for a CID regional command. As such, his input represents that from an Army LE perspective and should be expected to differ in that regard from the input previously

examined from the Army CI representative. The advantages the Army CID interviewee asserted exist in the CI and Intelligence and CI-LE organizational models are summarized in table 3.

Table 3. Advantages of Organizational Models per Army CID Interviewee

	CI and Intelligence	**CI-LE**
Identification	National intelligence connectivity	Efficient sharing of operational knowledge Increased operational understanding
Investigation		Enhanced situational awareness through information sharing
Neutralization		Efficient prosecution of all investigation types Army single point of investigative oversight

It is plain to see that this interviewee felt the advantages of a combined CI-LE organization outweighed the disadvantages, in his experience, of a CI and Intelligence model. This bias is of interest to this study because his views contradict the nature of his contemporary circumstances. As a Army CID officer, his present organization is separate from the Army CI organization. Where he feels that CI and LE functions should be combined, the Army CI representative's views examined earlier suggested the Army LE and CI organizations and functions should remain separate. A better understanding of this CID officer's perspective may be found through an analysis of the disadvantages of both organizational models which he proffered in his interview responses. Table 4 illustrates these disadvantages and underscores the bias already noted toward the CI-LE

organizational model. The discussion following table 4 examines the specific incidents that support this bias.

Table 4. Disadvantages of Organizational Models per Army CID Interviewee

	CI and Intelligence	**CI-LE**
Identification	Most CI information is over-classified leading to lack of sharing between LE/CI organizations Requires external relationships with LE organizations that are largely personality dependent No clear articulation of what should be shared between CI and LE organizations can lead to missed opportunities No visibility on interagency leads once they are exchanged	
Investigation	Requires external relationships with LE organizations that are largely personality dependent No clear articulation of what should be shared between CI and LE organizations can lead to missed opportunities	
Neutralization	Requires external relationships with LE organizations that are largely personality dependent	

It is clear from the table above the CID representative found more disadvantages with the current CI and Intelligence organizational construct in the Army. The interviewee based his opinions on specific cases and interchanges he had had with Army CI representatives. Citing that the lack of visibility on the furtherance of leads exchanged as one of the biggest problems, CID interviewee recalled examples that supported his

contentions. In summary, this interview displayed a shift from the parochial loyalties, observed in the CI representative's interview, to a concern the investigative organizational status quo in the Army requires re-examination and possibly improvement. Also of note is the fact the CID representative noted the single advantage inherent to the CI and Intelligence model currently in place is the connectivity to national intelligence architectures, a recurring theme in the interview with the Army CI representative. To resolve the discrepancy in satisfaction with the current Army organizational dispositions, this study also involved interviews of non-Army CI-LE investigators of a sister DoD investigative agency, the OSI.

Contrasting the two previous interviews which were of Army investigators in distinct and separate Army CI organizations and Army LE organizations, the Air Force Office of Special Investigations investigators perform both CI and LE from within the same organization. Unfortunately, inter-service coordination on CI cases is rare because of the differing and distinct equities involved within each service. Army CI protects Army forces, technologies and personnel whereas OSI maintains a similar mission focus for the same Air Force equities, a situation which rarely forces inter-service investigative cooperation. Therefore the OSI interview results show little in the way of comparing and contrasting the Army and Air Force organizational approaches because the OSI really do not have any exposure to the Army CI and Intelligence model other than a casual understanding that things are "different" in the Army. Nonetheless, the OSI interviews are extremely helpful in their objective criticisms of the CI-LE organizational construct from within which they operate. The results of these interviews were, predictably parochial in their assertion the CI-LE organizational model was superior to any other

proposition, but within that assertion each OSI interviewee conceded some key disadvantages of the CI-LE structure that ultimately assist in furthering the development of any useful answers to the fundamental questions of this thesis study. To best understand the perspectives presented in the OSI interviews, one must understand the OSI regional office composition contains LE and CI specialists who tend execute the majority of their work in their specialty, but can and will work in other areas if the office requires more manpower for a particular operation. The key advantages of the CI and Intelligence and CI-LE organizational models, as discovered in both OSI interviews, are summarized in a combined snapshot in table 5.

Table 5. Advantages of Organizational Models per OSI Interviewees

	CI and Intelligence	**CI-LE**
Identification		Opportunity for good sharing of information between CI and LE Single point of control for all Air Force investigations in region Investigators have some understanding of both CI and LE requirements
Investigation		Can counter domestic and foreign terrorism Flexible investigative manpower pool without sacrifice of lead investigator specialization Single point of control for all Air Force investigations in region
Neutralization		Efficient prosecution of all investigation types Internal collaboration opportunities for all operations

The themes of single point of investigative oversight and control, and enhanced opportunities for information sharing across the CI and LE investigative disciplines, are common thematic advantages of the CI-LE organizational model among both the Army and OSI investigators. But OSI interviewees also pointed out the CI-LE organizational model was not without its innate flaws. Table 6 below captures the essence of these flaws noted by the OSI agents.

Table 6. Disadvantages of Organizational Models per OSI Interviewees

	CI and Intelligence	**CI-LE**
Identification		Evolution of LE-centric or CI-centric culture Agents transferred from another office may be required to learn new specialty
Investigation		Multiple mission focus requires compromises in performance expectations Becomes critical to separate concurrent investigative efforts to avoid unnecessary distractions EO 12333 oversight issues require strict monitoring to preclude violation
Neutralization		

An understanding of the disadvantages of the CI-LE model as shown above indicate that, as with the CI and Intelligence model, the CI-LE model is not without its operational liabilities. It remains necessary, now that an examination of interview results is complete, to review the relevant findings concerning the two organizational models in

the literature available on this subject. To this end, a summary of the advantages and disadvantages inherent to both models and already referenced in this study are provided in tables 7 and 8 respectively.

Table 7. Advantages of Organizational Models per research conducted

	CI and Intelligence	**CI-LE**
Identification	Requires legal specialty in only intelligence law Connectivity to national intelligence	Efficient sharing of operational knowledge Enhanced situational knowledge
Investigation	Requires legal specialty in only intelligence law Access to intelligence analysis Can perform intelligence collection missions	Central oversight of all investigative responsibilities Reactive nature of CI compliments reactive nature of LE Limited EO 12333 concerns because of LE characteristics Can investigate foreign and domestic terrorists
Neutralization	Intelligence analysis can aid LE agencies	Efficient prosecution of all investigation types

Table 8. Disadvantages of Organizational Models per research conducted

	CI and Intelligence	**CI-LE**
Identification	Requires collaboration with external LE agencies that can be personality dependent Over classification of information No visibility over interagency leads	Proclivity for evolution of LE culture Requires diverse in-house specializations Limited national intelligence connectivity

Investigation	EO 12333 constraints Foreign terrorists only Reactive nature of CI conflicts with proactive nature of intelligence May require collaboration with external LE agencies that can be personality dependent	Limited intelligence analysis Requires legal expertise in both criminal and intelligence law
Neutralization	May require collaboration with external LE agencies that can be personality dependent	

As indicated by the tables 1-8, the Army CI organization suffers the most degradation in the identification and investigative categories. Without assigning any value or importance to any of the three categories, but treating them all as equally vital to strategic CI operations, the data collected suggests two of the three CI activities are significantly impaired. Interestingly, these same categories of identification and investigation, most plagued by cited disadvantages in the CI and Intelligence model, receive the most cited advantages in the CI-LE model. The causes of the degradation in the CI and Intelligence model are rooted in the executive orders and regulations that proscribe any Army intelligence collection or investigation of domestic terrorist activities, the reliance on external collaboration and contact to perform identification and investigation activities, and the inherent unreliability and personality-dependence that is the basis for these external contacts. Due to its affiliation with and subordination under the Army's Intelligence and Security Command, Army CI is considered an intelligence function where it is not considered an intelligence function in the OSI or NCIS. Therefore, such restrictions apply to the CI and Intelligence model and not to the CI-LE model.

In the research conducted, it is clear the benefits of an intelligence organization affiliation do not outweigh the burdens they apply to the ability of Army CI to accomplish its investigative mission across the full spectrum of the evolving contemporary threat. But this presentation of simple numbers of advantages versus disadvantages is not necessarily the most reliable analytical method for this data because it presumes that each advantage or disadvantage bears an equal weight or impact on the specific category of Army CI operations. Such a presumption cannot be maintained under scrutiny. Nevertheless, any analysis which attributed a relative weight to an advantage or disadvantage would run an even greater risk of invalidating any conclusions because of the purely subjective nature of assigning such weights. Instead, it may be more helpful to evaluate this data from the perspective of modern organizational design theory. This type of analysis will afford more insight into the actual fit of the CI and Intelligence organizational construct within the context of its requirements to identify, investigate, and neutralize foreign intelligence threats to the Army.

The most applicable organizational design model for this analysis is the sociotechnical system, in which all areas are seen as interrelated and changes in one area can effect changes in another (Harvey and Brown 2001). The sociotechnical system consists of five subsystems, the structural subsystem, the technical subsystem, the psychosocial subsystem, the goals and values subsystem, and the managerial subsystem (Harvey and Brown 2001). The structural subsystem embodies the rules of the organization; the technical subsystem refers to the skills and equipment necessary for the output of the system; the psychosocial subsystem can be characterized as the organizational culture; the goals and values subsystem includes the fundamental mission

and vision of the system; and the managerial subsystem is, in essence, the coherent integrator of all other subsystems toward a common mission (Harvey and Brown 2001). Using this model, and the characteristics of each subsystem, one can gain further insight into the nature of the disadvantages of the Army CI and Intelligence organizational model as documented in the field interviews. Each disadvantage can be catalogued into a subsystem and result in a more helpful, comprehensive analysis of the interview results.

The first disadvantage of the CI and Intelligence model listed in the identification category of Table 8 betrays a deficiency corresponding to the structural subsystem of the sociotechnical model. The rules of the organization, such as Executive Order 12333 (1981) and the FISA (1978), constrain the activities of CI agents and anyone affiliated with federal intelligence organizations to behave in certain ways as previously discussed. These rules require Army CI agents to collaborate with external organizations for investigative leads and authorities.

The second disadvantage of the CI and Intelligence model listed in the identification category of table 8 also betrays a deficiency corresponding to the structural subsystem of the sociotechnical model. The perceived over-classification of information is a result of compliance with applicable classification guides and regulations. These procedures are part of the rules of any intelligence organization, and therefore clearly fall into the realm of the structural subsystem.

The last disadvantage of the CI and Intelligence model listed in the identification category of table 8 illustrates a third deficiency corresponding to the structural subsystem of the sociotechnical model. The lack of any organic relationship between Army CI and Army CID leads to the lack of visibility of leads exchanged. A CI agent who passes a

criminal lead to CID will have no more knowledge of the outcome of that lead than the CID agent who passes an espionage lead to CI. That is not to say that any such knowledge is critical to the success of the overall Army investigative responsibility, but the lack of regulatory communication and feedback was perceived by the agent on the ground, in this study, as a disadvantage. In this case, the lack of rules, as opposed to the constraint of the rules, serves as the qualification for this disadvantage to be categorized as within the structural subsystem.

The first disadvantage of the CI and Intelligence model listed in the investigation category of table 8 illustrates another deficiency corresponding to the structural subsystem of the sociotechnical model. Affiliation of Army CI with an intelligence organization demands intricate oversight of all investigative activities to ensure compliance with Executive Order 12333 (1987), which specifies such oversight of intelligence organizations. This is clearly an instance when the rules of the organization serve as a constraint and a structural disadvantage according to the sociotechnical model.

The next disadvantage of the CI and Intelligence model listed in the investigation category of table 8 is linked to the previous disadvantage and similarly corresponds to the structural subsystem of the sociotechnical model. Because the implications of Executive Order 12333 effectively limit domestic intelligence collection to foreigners, unless special dispensation is granted, Army CI cannot freely investigate indications of domestic terrorism whereas sister service CI-LE organizations can investigate both under its dual authorities. Again, the rules specific to the CI and Intelligence model can be interpreted as a structural liability.

The subsequent disadvantage of the CI and Intelligence model listed in the investigation category of table 8 illustrates the only deficiency of the CI and Intelligence model that does not correspond to the structural subsystem of the sociotechnical model. Instead, the perceived antagonistic blend of the theoretical natures of CI and Intelligence within the same organization represent more of a technical disadvantage of the CI and Intelligence model. Because the reactive nature of CI requires a skill set that contrasts that required by the proactive nature of intelligence collection, the sociotechnical subsystem affected by this contrast is purely technical.

The final disadvantage of the CI and Intelligence model listed in the investigation category of table 8 illustrates another deficiency corresponding to the structural subsystem of the sociotechnical model, repeated from the identification category in the same table. As previously described, the need for external collaboration and the dysfunction possible because of the lack of rules governing these contacts, highlights a vulnerability that is rules-based and inherently impacts the structural subsystem of the sociotechnical model.

This same disadvantage of external collaboration is also repeated in the neutralization category of table 8, that category's only disadvantage.

As one reviews the comparative analysis above, attributing disadvantages cited from the field to sociotechnical subsystems, it becomes obvious the predominant disadvantage of the CI and Intelligence organization is firmly rooted in the structural subsystem of the sociotechnical model. Because the structural subsystem reflects the rules specific to an organization, one can infer any deliberate housing of CI and intelligence activities within a common organization in the United States will require

compliance with rules that serve to disadvantage that same organization. This postulate does not seriously contradict what this paper has already shown through prior discussions, in fact it further supports the analysis conducted in chapter 1 and chapter 2. In an effort to challenge this postulate further, an analysis is required of the data collected concerning the disadvantages of the CI-LE model. If such an analysis also demonstrated an overwhelming structural bias, it could be argued the postulate was not useful because it supported both organizational models. Fortunately the analysis of the CI-LE organization disadvantages shows a clear liability in the technical subsystem of the sociotechnical model, not the structural subsystem.

The first disadvantage of the CI-LE organization listed in the identification category of table 8 corresponds to the psychosocial subsystem of the sociotechnical model. The tendency for this type of hybrid organization to develop an LE-centric focus clearly refers to organizational culture, clearly the realm of the psychosocial subsystem.

The second disadvantage of the CI-LE organization listed in the identification category of table 8 corresponds to the technical subsystem of the sociotechnical model. Diverse in-house skill sets is plainly a technical concern.

The third and final disadvantage of the CI-LE organization listed in the identification category of table 8 also corresponds to the technical subsystem of the sociotechnical model. Limited connectivity to the national intelligence architecture was noted as a disadvantage in these times of global proliferation, espionage and terrorism. Without the proper equipment and commensurate skills to tap into national intelligence information concerning these threats, the CI-LE organization is at a serious disadvantage, and one that obviously is rooted in its technical subsystem.

The first disadvantage of the CI-LE organization listed in the investigation category of table 8 corresponds to the technical subsystem of the sociotechnical model. This disadvantage, having limited ability to conduct or access to intelligence analysis, can hamper the effectiveness of the CI-LE organization.

The second and final disadvantage of the CI-LE organization listed in the investigation category of table 8 also corresponds to the technical subsystem of the sociotechnical model. Because the nuances of law can have such tremendous ramifications in the prosecution of crimes in a democracy, requiring a single organization to be proficient in both criminal law and intelligence law is both compelling and difficult. This difficulty correlates to a disadvantage that can only be obviated through specific skills of specific organizational members. In other words, the requirement to be proficient in not one but two disciplines of federal law is a disadvantage within the technical subsystem of the CI-LE organization.

By reviewing the above disadvantages of the CI-LE organization and their attributed sociotechnical subsystems and comparing these disadvantages to those of the CI and Intelligence organization, one can see a distinct difference. These differences in subsystem are presented below in table format, listed in each category in the order discussed in this paper and correlating to the same ordinal position in table 8.

Table 9. Sociotechnical Attributes of Disadvantages from Table 8

	CI and Intelligence	**CI-LE**
	Structural	Psychosocial
	Structural	Technical
Identification	Structural	Technical

	CI and Intelligence	CI-LE
Investigation	Structural Structural Technical Structural Structural	 Technical Technical
Neutralization	Structural	

The visual collation of the sociotechnical attributes of disadvantages from both organizational constructs that were assessed shows a clear bias toward structural deficiencies in the CI and Intelligence organization, and a clear bias toward technical deficiencies in the CI-LE organization. Because the bias was not the same for both constructs, it is reasonable to further assert the validity of the postulate previously proposed. The deliberate housing of CI and intelligence activities within a common organization in the United States will require compliance with rules that serve to disadvantage that same organization's operations. And this analysis has shown the preponderance of this deleterious impact will be in the identification and investigation categories of CI activity.

To further corroborate this postulate and the use of the sociotechnical model as its basis, an examination of the advantages listed in table 7 show similar contrasts in subsystem strengths. Again, sociotechnical attributes are listed in ordinal fashion to correlate with the respective advantage in table 7.

Table 10. Sociotechnical Attributes of Advantages from Table 7

	CI and Intelligence	**CI-LE**
Identification	Technical Technical	Structural Managerial
Investigation	Technical Technical Structural	Managerial Technical Structural Structural
Neutralization	Goals and Values	Managerial

Before developing any broad conclusions from this data and analysis, it remains necessary to highlight the limitations of this research. The limitations fall into two general categories, sample and data.

One of the most obvious limitations of the sample in this study is that it was non-probability based. Interviewees were not selected at random, but by virtue of their position, namely regional supervision or command of any federal organization with an official CI investigative mission. It is possible a more probability-based sample would provide more data for analysis, but efforts were made to limit inputs to those that would be seasoned with experience. Clearly a probationary or intern agent would not possess the breadth of experience to provide detailed responses sufficient for this study. Nevertheless, the sample was not probability based and this study acknowledges the vulnerabilities normally associated with such samples.

Dovetailing with the nonprobability nature of the sample was the very small size of this sample. Because this study limited its solicitations to specific CI and LE positions of at least regional scope, this criteria sharply limited the population and frame available. Furthermore, sampling error attributable to non-respondents further reduced the frame. Not only did eligible FBI and NCIS offices decline participation in this study, additional efforts to garner participation from CI supervisors at the national level of the Army were similarly declined. As a result, the study concluded with only four successful interviews. Obviously, more interviews will be necessary to fully substantiate the data and relevant conclusions of this study.

Respondent error accounts for the final limitation associated to the sample limitations. Because the final sample was much smaller than anticipated, respondent error was greatly magnified, as characterized by the limited cross-service experiences of the respondents. In fact, there was only one respondent with any experience with more than a single service. One of the OSI respondents disclosed having served as a CID agent previously. While such experience was helpful to this study, previous work with Army CI, in any capacity would have been more preferred. With a larger sample, the probability of gaining cross-service experiential insights would have greatly increased.

Finally, the nature of the data collected did not present any opportunity for quantitative analysis, another facet of this study which may be perceived as a limitation. In fact, all data collected was qualitative in nature, followed by subjective assessment. Future research on this topic may consider a more quantitative approach in order to further refine findings.

Despite the limitations ascribed to this study, there was real progress made in understanding the subtle intricacies of the Army CI organizational anomaly. Based on an analysis of the literature available and the data collected from the field, resulting conclusions should provide some utility to those eager to grapple with the challenges of conducting strategic, domestic Army CI operations in the twenty-first century. These conclusions, as well as some recommendations, are presented in the following chapter.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Based on the analysis of data gathered in this study, the Army's CI and Intelligence organization, which represents the anomalous status quo, has significant deficiencies in the structural subsystem which inhibit its full exploitation of the recent erosion of barriers between FISA and criminal investigative procedures. These structural deficiencies are most pronounced in the CI activities characterized as identification and investigation of the threat. The alternative organizational construct, the CI-LE model, manifested fewer liabilities from the data collected. The preponderance of these liabilities affected the technical subsystem of the CI-LE organizational model. Therefore, neither organizational construct is perfect, but clearly the Army's status quo for conducting strategic, domestic CI has significant shortfalls which should be further studied. In the event the conclusions of this study are heeded, the following recommendations are presented concerning any intervention in the psychosocial, goals and values, and structural subsystems of the current Army CI organization. These recommendations are based upon the literature reviewed, data collected, and observations made during the course of this study.

The psychosocial subsystem of Army strategic CI organization can be characterized as strong. This sentiment was found in literature (McDonough 1987) as well as during the conduct of the interview of the Army CI representative. During the interview it became apparent the interviewee prided himself on each CI victory because of an organizational perception that the policies and procedures that safeguard Fourth

Amendment rights can only be interpreted to as defy any CI accomplishments at all. This structural fallibility of the CI and Intelligence construct was delineated in chapter 4. In addition to this feeling of unity in their mission of neutralizing espionage and terrorism despite the odds, all Army CI agents are issued a badge and credentials that identify them as Special Agents of Army Intelligence, and they are allowed to wear civilian clothes in order to blend in with activities outside of Army installations (DA 1984). This lack of uniform and the small icon of the badge are symbols that set CI agents apart from the rest of the Army and reinforce the culture of the Army CI organization. Because the psychosocial subsystem is so strong and a guarded source of pride for the organization, any attempt to intervene in a way that would depreciate this subsystem should be expected to provoke strong resistance. Similar resistance should be expected if the goals and values subsystem is likewise threatened.

The Army CI community believes fiercely in its mission of protecting Army forces, technologies and secrets from espionage and foreign terrorist threats. This determination and resolve were apparent in the Army CI representative interview and characterize the strength of the goals and values subsystem within the Army CI organization. This commitment to a common vision of defense was reinforced during the interview when the Army CI respondent asserted that many times only he had the necessary shred of intelligence, because of access, to help in other agencies operations. Any intervention that blurs the mission or weakens its importance in any way will challenge this mature goals and values subsystem and possibly provoke undercurrents of resistance from Army CI members.

The structural subsystem represents the intricate collection of rules, legislation and directives that guide the conduct of Army CI investigative functions. As discussed at the beginning of this chapter, these guides in the Army CI organization also contribute to the culture of the organization and help to define it among its members and differentiate it from its competitors or sister services. This strong linkage between subsystems in the same organization is a normal, expected phenomenon of the sociotechnical system. In fact it represents the model's unique relevancy (Harvey and Brown 2001). Unfortunately for the Army CI organization these strong links exist between a subsystem that requires no change (psychosocial), and one this study has determined does require alteration. It should be expected that any alterations to the structural subsystem of the Army CI organizational status quo will provoke similar reactions in the psychosocial subsystems, and these reactions will likely be characterized by resistance. Despite the fact this study revealed significant liabilities of the CI and Intelligence organizational construct, the Army's CI status quo, Army CI agents appear perfectly content within their structural subsystem. During the field interview for this study, the Army CI interviewee was able to regurgitate the titles and numbers of numerous specific Department of Defense and Army regulations that supported his contentions. His dedication to the process, demonstrated during this interview, is reinforced in other literary sources (Bunchner 1977; Herrington 1999; McDonough 1987; Mendelsohn 1989) that defined the theoretical and practical differences between CI, LE and intelligence. Because the Army CI agent's inherent bond with the structural subsystem of his/her context, the clear assimilation of the psychosocial subsystem, and the established tie between the structural and psychosocial subsystems within the organizational framework, it should be expected that any intervention that

threatens to alter the legal and procedural framework of the Army CI structural subsystem should expect to meet some level of challenge and most probably resistance.

If such organizational change is deemed necessary for Army CI to undertake, this study should be re-assessed for relevancy and further data collected to mitigate the limitations of the research noted in chapter 4. Nevertheless, the implications of change to the Army CI organizational status quo will remain controversial and painful for many. The sociotechnical recommendations of this study may assuage the fears of intervention by highlighting the discreet piles of tinder in the organization, but these recommendations are no substitute for the deliberate planning that will be necessary to secure the tinder before it can ignite and ensure continued vitality within Army CI. Coming to grips with the new challenges and threats of the twenty-first century will require changes to the structural subsystem of the organization, changes which will probably affect other subsystems as well. But the pain involved in intervention and change is certainly better than lapsing into irrelevancy as an obsolete anomaly.

REFERENCE LIST

Air Force Office of Special Investigations. 2000. *Fact sheet*. available from: http://www.af.mil/news/factsheets/Air_Force_Office_of_Special_I.html; Internet; accessed 1 December 2002.

Antiterrorism and Effective Death Penalty Act. Statutes at Large. 1996.

Ashcroft, J. 2002. *News conference transcript regarding decision of foreign intelligence surveillance court of review*. available from: www.usdoj.gov/ag/speeches/2002/111802fisanewsconference.htm; Internet; accessed 1 December 2002.

Brookings Institution. 2002. *Protecting the American homeland*. Washington D.C.: Brookings Institution Press.

Buncher, John. 1977. *The CIA and the security debate: 1975-1976*. New York, NY: Facts on File Inc.

Daft, Richard. 2001. *Organization theory and design*. Cincinnati, OH: South-Western College Publishing.

Defense Security Service. 1999. *1999 technology collection trends in the US defense industry*. available from: http://www.dss.mil/cithreats/99dss_trends.html; Internet; accessed 2 December 2000.

Defense Security Service. 2000. *2000 technology collection trends in the US defense industry*. Washington DC: Defense Security Service.

Department of the Army. 1984. *US Army intelligence activities. Army regulation 381-10.*

Department of Defense (2000). *Joint publication 2-0: Doctrine for intelligence support to joint operations*.

Economic Espionage Act. Statutes at Large. 1996. H.R. 3723.

Executive Order Number 12333, 50 USC. § 401 et seq. 1981.

Federal Bureau of Investigation. 2002. *Headquarters and programs*. available from: http://www.fbi.gov/hq.htm; Internet; accessed 1 December 2002.

Foreign Intelligence and Surveillance Act, 50 USC. §§ 1801-1811, 1821-1829, 1841-1846, 1861-62, 1978.

Freeh, Louis. 1998. *Congressional statement on threats to US national security*. available from: http://www.fbi.gov/congress/congress98/threats.htm; Internet; accessed 1 December 2002.

Hamre, John. 2000. *A strategic perspective on US homeland defense: Problem and response*. Edited by M. G. Manwaring. *To insure domestic tranquility, provide for the common defense.* Carlisle, PA: Strategic Studies Institute.

Harvey, Don, and Donald Brown. 2001. *An experiential approach to organizational development*. Upper Saddle River, New Jersey: Prentice Hall.

Herrington, Stuart. 1999. *Traitors among us*. Novato, CA: Presidio Press.

House of Representatives Permanent Select Committee on Intelligence. 1996. *IC21: the intelligence community in the 21st century*. available from: http://www.access.gpo.gov/congress/house/intel/ic21/ic21013.html; Internet; accessed 1 December 2002.

House of Representatives Permanent Select Committee On Intelligence. 2002. *Counterterrorism intelligence capabilities and performance prior to 9-11*.

Intelligence and Security Command. 2002. *Mission and vision*. available from: http://www.inscom.army.mil/mission.asp; Internet; accessed 1 December 2002.

Markle Foundation Task Force. 2002. *Protecting America's freedom in the information age*. New York, New York: Markle Foundation.

McDonough, Thomas. 1987. *Reorganization of US Army counterintelligence and criminal investigative functions* (Masters thesis, US Army Command and General Staff College, 1987). (Distribution restricted due to content), Alexandria, VA: Defense Technical Information Center.

McNamara, Francis. 1985. *US counterintelligence today*. Washington DC: The Nathan Hale Institute.

Mendelsohn, John. 1989. *Covert warfare: The history of the counter intelligence corps (CIC).* New York, NY: Garland Publishing.

Mueller, Robert. 2002. *Congressional statement on a new FBI focus*. available from: http://www.fbi.gov/congress/congress02/mueller062102.htm; Internet; accessed 1 December 2002.

National Counterintelligence Center. 2002. *The presidential directive on CI-21*. available from: http://www.nacic.gov/pubs/online/ci-21.html; Internet; accessed 1 December 2002.

Naval Criminal Investigative Service. 2002. *NCIS activities*. available from: http://www.ncis.navy.mil/activities; Internet; accessed 1 December 2002.

Pratt, Ginger. 2002. *The 902d military intelligence group and homeland security*. In Military Intelligence Professional Bulletin, Jul-Sep 2002, Vol. 28, Issue 3.

Rindskopf-Parker, Evelyn. 2000. Edited by C. W. Pumphrey. *Transnational threats: Blending law enforcement and military strategies.* Carlisle, PA: Strategic Studies Institute.

Szady, Donald. 2002. *Statement before the senate judiciary committee on changes the FBI is making to the counterintelligence program.* available from http://www.fbi.gov/congress/congress02; Internet; accessed 1 December 2002.

Patriot Act. *Statutes at Large*. 2001. H.R. 3162.

Thomas, Steven. 1983. *The US intelligence community*. Latham, MD: University Press of America Inc.

United States Army Criminal Investigation Command (2002). *Mission statement*. available from: http://www.belvoir.army.mil/cidc/mission1.htm; Internet; accessed 1 December 2002.

United States General Accounting Office. *FBI intelligence investigations – coordination within justice on counterintelligence criminal matters is limited*. Washington, 2001.

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
US Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/OCA
825 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

LTC Y. Doll
Center for Army Leadership
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

LTC J. Burcalow
Center for Army Tactics
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

Dr. R. Spiller
Center for Military History
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 6 June 2003

2. Thesis Author: MAJ Merle V. Bickford

3. Thesis Title: The Organizational Anomaly of US Army Strategic Counterintelligence

4. Thesis Committee Members: _____

Signatures: _____

_____

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

(A) B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

EXAMPLE

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
Direct Military Support (10)	/	Chapter 3	/	12
Critical Technology (3)	/	Section 4	/	31
Administrative Operational Use (7)	/	Chapter 2	/	13-32

Fill in limitation justification for your thesis below:

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
	/		/	
	/		/	
	/		/	
	/		/	
	/		/	

7. MMAS Thesis Author's Signature: _____

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals).

STATEMENT B: Distribution authorized to US Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the US Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation - release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a US military advantage.

STATEMENT C: Distribution authorized to US Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and US DoD contractors only; (REASON AND DATE). Currently most reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to US Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).